## REMARKS

Claim Changes

Claim 16 is amended to recite "distributing the encrypted first key, wherein the distributed first key updates the cryptographic key." These changes are based at least on FIG. 2 and the accompanying description on page 10, lines 9-11, and 21-23 of the specification as filed. Thus, no new matter is added.

No amendment made is related to the statutory requirements of patentability unless expressly stated herein. No amendment is made for the purpose of narrowing the scope of any claim, unless Applicants argue herein that such amendment is made to distinguish over a particular reference or combination of references. Any remarks made herein with respect to a given claim or amendment is intended only in the context of that specific claim or amendment, and should not be applied to other claims, amendments, or aspects of Applicants' invention.

Rejection of claims 1-7 and 10-15 under 35 U.S.C. § 103 (a) as being unpatentable over "Handbook of Applied Cryptography" (Menezes) in view of US 6,044,350 (Weiant)

Applicants respectfully traverse the rejection of claims 1-7 and 10-15. Reconsideration is respectfully requested.

Applicants respectfully submit that the Menezes reference or the combination of Menezes and Weiant does not teach or suggest all the claim limitations as set forth in independent claims 1 and 10. Specifically, claim 1 recites "a first key for performing asymmetric operations at a first rate," "a second key for performing an asymmetric cryptographic processing operation to update the first key," and "the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate." These specific limitations are not taught or suggested in Menezes or the combination of Menezes and Weiant.

Menezes discloses a key layering technique for distributing cryptographic keys when confidentiality of the private and symmetric keys must be preserved. The key layering technique consists of master keys at the highest level, key-encrypting keys, and data keys. The data keys are used to perform cryptographic operations on user data. The asymmetric signature private keys considered as data keys are usually longer-term keys. The key-encrypting keys are encryption public keys used for key transport or storage of other keys. The key-encrypting keys are used as long-term keys that have higher time period over which it is valid.

Applicants respectfully disagree with the statement in item 5, page 3, of the Office Action dated April 9, 2008 that "Menezes et al. teaches an asymmetric cryptographic processing system…comprising: A first key for performing asymmetric operations at a first rate…(Page 552, step 3, data keys, provide cryptographic operations on user data, tend to be short-term keys)." Office Actions appears to equate Applicants' "first key" with Menezes's "data keys." However, Menezes discloses that the data keys considered as asymmetric signature private data keys are usually longer-term data keys. Further in Meneze's, the longer-term key is defined as the time period over which the data key is valid. See page 553, lines 3-5 of Menezes. Thus, Meneze discloses the time period (long-term or short-term) over which the data key is valid, and makes no mention of the rate (frequent or infrequent use) at which the data key is used for performing asymmetric operations. In contrast, Applicants' claim recites "a first key for performing asymmetric operations at a first rate."

Further, Office Action, in item 5, page 3 states that the "Menezes et al. teaches an asymmetric cryptographic processing system…comprising…A second key for performing an asymmetric cryptographic processing operation to update the first key (page 552, step 2, key-encrypting keys)." Office Action appears to equate Applicants' "second key" with Menezes's "key-encrypting key." However, Menezes discloses a key layering technique for distributing the cryptographic keys when confidentiality of the private and symmetric keys must be preserved. Further, Menezes discloses that the key-encrypting keys are used for key transport or storage of other keys. Thus, Menezes, at most, uses the key-encryption key to transport or distribute other keys, and not for updating the data keys at a particular rate. In contrast, Applicants' claim recites "a second key for performing an asymmetric cryptographic processing operation to update the first key."

Additionally, Menezes's simply discloses that the key-encrypting key is used to transport other keys, and also discloses a time period over which the key-encrypting key is valid. However, Menezes makes no mention of the rate at which the key-encryption key is used to update the data key (equated to Applicants' first key), and also makes no mention of the rate at which the data key is updated is less than the rate at which the data key is used for performing asymmetric cryptographic operations. In contrast, Applicants' claim recites "the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and that requires a second cryptographic processing time greater than the first cryptographic processing time."

Further, the Weiant reference describes a system for a general-purpose computer that includes a digital certificate meter to certify an electronic commerce purchase by a user. For each purchase, the user interacts with the digital certificate meter to select a service rate that the system adds to the purchase to indemnify the purchase for a given amount. The user selects the service rate from a table of security and indemnification rates that the system displays to the user. However, Weiant also fails to describe the above mentioned claim limitations. Therefore, the Menezes reference or the combination of Menezes and Weiant does not teach or suggest the above mentioned claim limitations as recited in Applicants' claim 1, so the Applicants respectfully request withdrawal of the rejection of claim 1 under 35 U.S.C 103.

Regarding independent claim 10, Applicants respectfully submit that the above discussed arguments apply equally to the limitations of claim 10. Applicants therefore respectfully request withdrawal of the rejection of claim 10 under 35 U.S.C 103.

Dependent claims 2-7 and 11-15 depend from, and include all the limitations of independent claims 1 and 10. Therefore, Applicants respectfully request the reconsideration of dependent claims 2-7 and 11-15 and request withdrawal of the rejection.

Rejection of claims 16-19 under 35 U.S.C. § 103 (a) as being unpatentable over US 5,850,443 (Van Oorschot) in view of US 5,796,840 (Davis)

Applicants have amended the claims to clarify the invention. Applicants therefore respectfully request reconsideration of the rejection of claims 16-19 under 35 U.S.C. § 103(a) as being unpatentable over Van Oorschot in view of Davis.

The Office Action on page 8, line 17 to page 9, line 6 states "Van Oorschot et al. does not teach wherein the first key updates the cryptographic key; and wherein the cryptographic key, the first key, and the second key encrypt and decrypt data using a similar class of algorithm to encrypt and decrypt data." In the Office Action, it is acknowledged that Van Oorschot does not disclose this but that "Davis teaches wherein the first key updates the cryptographic key (col. 6, lines 7-27); and wherein the cryptographic key, the first key, and the second key encrypt and decrypt data using a similar class of algorithm to encrypt and decrypt data (fig. 7, all use asymmetric key for encryption and decryption)."

Davis discloses a method for providing a secured communications between a system incorporating a cryptographic semiconductor device and a device in remote communications with the system. The cryptographic semiconductor device includes a hardware agent placed onto a certification system which establishes an electrical connection to the hardware agent and the certificate system. The certificate system includes a storage device for storage of prior generated public keys. Further, the hardware agent initiates a configuration sequence which is further used by a random number generator to generate a specific public/private key pair. The generated public/private key pair is then sent to the certification system where the key pair is compared to the storage device of the prior generated public keys, and then updated with this new public/private key pair. Thus, in Davis, the stored key pair is updated by the internally generated public /private key pair, and not updated by the distributed encrypted key pair received from the transmitter. In contrast, Applicants' amended claim recites "distributing the encrypted first key, wherein the distributed first key updates the cryptographic key."

Therefore, the combination of Van Oorschot and Davis does not teach or suggest the above mentioned claim limitation as recited in Applicants' amended claim 16, so the Applicants respectfully request withdrawal of the rejection of claim 16 under 35 U.S.C 103.

Dependent claims 17-19 depend from, and include all the limitations of independent claim 16. Therefore, Applicants respectfully request the reconsideration of dependent claims 17-19 and request withdrawal of the rejection.

## Conclusion

Applicants respectfully request that a timely Notice of Allowance be issued in this case. Such action is earnestly solicited by the Applicant. Should the Examiner have any questions, comments, or suggestions, the Examiner is invited to contact the Applicants' attorney at the telephone number indicated below.

Please charge any fees that may be due to Deposit Account 502117, Motorola, Inc.

Respectfully submitted,
ERIC J. SPRUNK et al.

Date: August 15, 2008

BY: /Stewart M. Wiener/
Stewart M. Wiener
Registration No. 46,201
*Attorney for Applicants*

MOTOROLA, INC.
101 Tournament Drive
Horsham, PA 19044
Telephone: (215) 323-1811
Fax: (215) 323-1300